CLAIMS:

1-6. (**Canceled**).

7. (**Original**) A wireless network intrusion detection and prevention system, comprising:

a plurality of monitor agent applications installed on a plurality of wireless network devices for collecting wireless event data from a wireless network;

a plurality of wireless access points for providing access to the wireless network for the plurality of wireless network devices;

a secure communications link for providing secure communications between the plurality of wireless network devices and other components of the wireless network intrusion detection and prevention system;

a cooperative decision engine for collecting wireless event data from the plurality of monitor agent applications installed on the plurality of wireless network devices the plurality of wireless network devices and the plurality of wireless access points, for screening the wireless event data for normal events and abnormal events, for sending decision data to a response initiator adaptive feedback engine based on processing of the normal event and abnormal events and for receiving state data from the response initiator adaptive feedback engine;

a fuzzy association engine including an adaptive learning detection system for adaptively detecting abnormal events and preventing similar abnormal events based on wireless event data received from the cooperative decision engine; and

a response initiator adaptive feedback engine for receiving decision data from the

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

cooperative decision engine, for sending state information to the cooperative decision engine, for sending response control information to a plurality of wireless access points through the secure communications link, and for maintaining a running mistrust level for the plurality of wireless network devices and the plurality of wireless access points on the wireless network.

8. (**Original**) The wireless network intrusion detection and prevention system of Claim 7 further comprising a plurality of smart wireless antenna subsystems associated with the plurality of wireless access points.

9. (**Canceled**).

10. (**Original**) The wireless network intrusion detection and prevention system of Claim 7 wherein the secure communications link includes wireless encrypted communications.

11. (**Original**) The wireless network intrusion detection and prevention system of Claim 7 wherein the cooperative decision engine includes a wireless event anomaly profiler, a normal wireless event profile database and a set of wireless event misuse rules.

12. (**Original**) The wireless network intrusion detection and prevention of Claim 7 wherein the response initiator adaptive feedback engine sends alarms and wireless event log files to a network administrator, and receives manual control from the network administrator.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

13. (**Original**) The wireless network intrusion detection and prevention of Claim 7 wherein the running mistrust level of the response initiator adaptive feedback engine includes a plurality of mistrust levels and a plurality of associated response mechanisms.

14. (**Original**) The wireless network intrusion detection and prevention of Claim 13 wherein the plurality of response mechanisms include a plurality of security protection suites.

15. (**Original**) The wireless network intrusion detection and prevention of Claim 14 wherein the plurality of security protection suites include an encryption method, a secure hash method, a Diffie-Hellman group method, a method of encryption key authentication and a mistrust level decrement interval.

16. (**Original**) The wireless network intrusion detection and prevention of Claim 13 wherein the plurality of associated response mechanisms includes continuing normal operation, cycling between a plurality of security protection suites, switching radio frequency bands, or excluding a wireless network device or wireless access point from the wireless network and requesting re-authentication and re-login of the wireless network device or wireless access point on the wireless network.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

17. (**Original**) The wireless network intrusion detection and prevention of Claim 7 where the decision data includes X, Y coordinates for a physical location of a monitor agent application, wireless network or device, wireless access point where an wireless anomaly event has been detected, a confidence level in the detected wireless anomaly event, a type of wireless anomaly and a mistrust level decrement value from a security protection suite.

18. (**Original**) The wireless network intrusion detection and prevention of Claim 15 where a mistrust level associated with the mistrust level decrement value is calculated with:

$$M_{new} = M + \alpha\beta - M_{dec\_val},$$

where M_{new} is a new mistrust level, M is an old mistrust level, α is a confidence level in a detected anomaly, β is a weight assigned to a type of anomaly and, M_{dec_val} is a mistrust level decrement value.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

19. (**Original**) An integrated wireless intrusion detection and prevention security system, comprising:

a smart wireless antenna subsystem at a physical layer in a wireless network infrastructure on a wireless network for detecting a direction of arrival of a wireless signals from a selected wireless network device from a set of a plurality of wireless network devices on a wireless smart antenna subsystem associated with a wireless access point, for analyzing the direction of arrival to determine whether the detected signal is from a rouge wireless network device, and if so, creating a wireless beamform and directing the wireless signal from the rouge wireless network device to a null area in the wireless signal pattern being transmitted by the wireless access point; and

a wireless network intrusion detection and prevention system at a data link layer in the wireless network infrastructure on the wireless network for collecting wireless event data from the wireless network, analyzing the collected wireless event data for normal and abnormal wireless events, and for providing network security response controls to the plurality of wireless network devices and the wireless access point on the wireless network based on the analyzed collected wireless event data.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

20. (**Canceled**).

21. (**Original**) The integrated wireless intrusion detection and prevention security system of Claim 19 wherein the wireless network intrusion detection and prevention system comprises:

a plurality of monitor agent applications installed on a plurality of wireless network devices for collecting wireless event data from a wireless network;

a plurality of wireless access points for providing access to the wireless network for the plurality of wireless network devices;

a secure communications link for providing secure communications between the plurality of wireless network devices and other components of the wireless network intrusion detection and prevention system;

a cooperative decision engine for collecting wireless event data from the plurality of monitor agent applications installed on the plurality of wireless network devices the plurality of wireless network devices and the plurality of wireless access points, for screening the wireless event data for normal events and abnormal events, for sending decision data to a response initiator adaptive feedback engine based on processing of the normal event and abnormal events and for receiving state data from the response initiator adaptive feedback engine;

a fuzzy association engine including an adaptive learning detection system for adaptively detecting abnormal events and preventing similar abnormal events based on wireless event data received from the cooperative decision engine; and

a response initiator adaptive feedback engine for receiving decision data from the

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

cooperative decision engine, for sending state information to the cooperative decision engine, for sending response control information to a plurality of wireless access points through the secure communications link, and for maintaining a running mistrust level for the plurality of wireless network devices and the plurality of wireless access points on the wireless network.

22. (**Original**) A method for wireless intrusion detection and prevention, comprising:

detecting a direction of arrival of a wireless signal from a wireless network device on a smart wireless antenna subsystem associated with a wireless access point;

analyzing the direction of arrival to determine whether the wireless signal is from a rouge wireless network device, and if so,

adaptively creating a wireless beamform and directing the wireless signal from the rouge wireless network device to a null area in a wireless signal pattern being transmitted by the wireless access point.

23. (**Original**) The method of Claim 22 further comprising a computer readable medium having stored therein instructions for causing a processor to execute the steps of the method.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

24. **(Canceled).**

25. **(Original)** A method for wireless intrusion detection and protection security, comprising:

maintaining plural mistrust levels for a plurality of wireless signals for a plurality wireless network devices and for a plurality of wireless access points on a wireless network by a wireless security system;

detecting a wireless signal for a wireless event for a selected wireless network device or selected wireless access point on a smart wireless antenna subsystem;

determining a mistrust level for the detected wireless signal via the wireless security system using decision data created on the wireless security system from the detected wireless signal from the smart wireless antenna subsystem;

comparing the determined mistrust level to a mistrust level stored for the plural wireless signals for the plural wireless network devices and plural wireless access points; and

applying a selected security response control from the wireless security system based on the determined mistrust level to selected wireless network device or wireless access point.

26. **(Original)** The method of Claim 25 further comprising a computer readable medium having stored therein instructions for causing a processor to execute the steps of the method.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

27. (**Original**) The method of Claim 25, wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events.

28. (**Original**) The method of Claim 27, wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events in association with an adaptive learning detection system that collects and analyzes normal wireless events and abnormal wireless events over a time period T using a neural network that is adaptively and dynamically updated based on new detected wireless signals for normal wireless events and abnormal wireless events.

29. (**Original**) The method of Claim 25 wherein the neural network includes a Back Propagation Neural Network with positive training created with new detected wireless signal data.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

30. **(Original)** The method of Claim 25 wherein the Back Propagation Neural Network includes a training vector:

$(SS_{Cn}, X_p, Y_p, X_{Cn}, Y_{Cn})$,

where SS_{Cn} a detected wireless signal strength measured at an associated wireless access point P for a selected wireless network device C_n in a particular position (X_{Cn}, Y_{Cn}) and where X_p, is an X location of the selected wireless access point P, Y_p, is a Y location of the selected wireless access point P and X_{Cn}, Y_{Cn} are X,Y coordinates of the selected wireless network device.

31. **(Original)** The method of Claim 25 wherein the decision data in the step of determining a mistrust level includes X,Y coordinates for a wireless network device or a wireless access point, a confidence level for the detected wireless signal, a type of wireless signal anomaly and mistrust level decrement interval from a security protection suite.

32. **(Original)** The method of Claim 25 wherein step of applying a selected security response control includes cycling among a plurality of security protection suites, switching wireless bands, requiring re-authentication and/or re-identification, forcing the selected wireless network device or wireless access point off the wireless network.

33. **(Original)** The method of Claim 32 wherein the plurality of security protection suites include an encryption method, a secure hash method, a Diffie-Hellman group method, a method of encryption key authentication and a mistrust level decrement value.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751

34. (**Original**) The method of Claim 25 wherein step of applying a selected security response control includes cycling among a plurality of security protection suites as mistrust level is changed for a selected wireless network device or a wireless access point based on the determined mistrust level.

35. (**Original**) The method of Claim 25 wherein step of applying a selected security response control includes directing the selected wireless network device or wireless access point to a wireless null in a wireless signal pattern with the smart wireless antenna subsystem.

36. (**Original**) The method of Claim 25 wherein the smart wireless antenna subsystem operates at physical layer in a wireless network infrastructure on the wireless network.

37. (**Original**) The method of Claim 25 wherein the wireless security system operates at data-link layer or higher layers in a wireless network infrastructure on the wireless network.

LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603
TELEPHONE (312) 332-3751